POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Static Analysis for Malware Detection**
Jméno autora:	**Štěpán Dvořák**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	Ondřej Tichý
Pracoviště oponenta práce:	Ústav teorie informace a automatizace, AV ČR

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — náročnější

Hodnocení náročnosti zadání závěrečné práce.

Zadání hodnotím jako náročné a velmi ambiciózní s množstvím vlastní práce a přidané hodnoty.

Splnění zadání — splněno

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Zadání považuji bez výhrad za splněné.

Zvolený postup řešení — vynikající

Posuďte, zda student zvolil správný postup nebo metody řešení.

Student zvolil správný postup a dostatečně zdůvodnil každý krok svého řešení problému.

Odborná úroveň — A - výborně

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Student prokázal výborné znalosti a dovednosti ve studované problematice. V oboru se dobře orientuje a dokázal využít a propojit dostupné přístupy. Tyto přístupy nepoužívá bezmyšlenkovitě, ale je si vědom různých limitů a omezeních, které jsou v práci diskutovány i testovány. Předložené výsledky jsou porovnatelné se state-of-the-art metodami a jedná se tedy o velmi kvalitní výsledek.

Formální a jazyková úroveň, rozsah práce — A - výborně

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Práce je psána v anglickém jazyce a její čitelnost je velmi dobrá, na žádné zásadní jazykové nebo typografické chyby jsem nenarazil. Jako drobnou výtku bych uvedl pouze použití zkratek ještě před jejich zavedením (např. TPR a FPR).

Výběr zdrojů, korektnost citací — A - výborně

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Student cituje množství článků z kvalitních konferencí a časopisů a několik zdrojů online, celkem 32 citací, což považuji za dostatečné. Citační etika je dodržena a citace jsou úplné (s výhradou k citaci [21], kde se jedná o článek č. 4, nikoliv stranu 4, stran má článek celkem 7, ale to je drobnost).

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Student v rámci práce vytvořil a otestoval metodu, jejíž výsledky jsou srovnatelné se state-of-the-art metodami a která má potenciál k dalším vylepšením.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Předložená práce je na vysoké úrovni jak po stránce formální, tak po stránce obsahové. Student si osvojil velké množství znalostí a dovedností, které aplikoval na statickou klasifikaci malwaru. Výsledky, kterých dosáhl, jsou kvalitní a mají potenciál pro další zlepšení.
V práci je využit jako klasifikátor gradient boosting decision tree, konkrétně lightGBM algoritmus. Tento algoritmus, jak je popsáno v práci, má mnoho parametrů. Z práce není zcela jasné, jaké nastavení parametrů je doporučené a které změny způsobí potíže a které pouze malou změnu v kvalitě výsledků. Můžete okomentovat, která nastavení jsou upravena a která je naopak lepší neměnit a proč tomu tak je?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm A - výborně.

Datum: 04.06.18 Podpis: